Int. J. Communications, Network and System Sciences, 2015, 8, 552-566
Published Online December 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.813050

Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)

Arif Sari[1], Onder Onursal[2], Murat Akkaya[1]

[1]Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
[2]Department of Management Information Systems, European University of Lefke, Lefke, Cyprus
Email: arifsari@gau.edu.tr, oonursal@eul.edu.tr, muratakkaya@gau.edu.tr

Received 22 April 2015; accepted 27 December 2015; published 30 December 2015

Abstract

There is a significant increase in the rates of vehicle accidents in countries around the world and also the casualties involved ever year. New technologies have been explored relating to the Vehicular Ad Hoc Network (VANET) due to the increase in vehicular traffic/congestions around us. Vehicular communication is very important as technology has evolved. The research of VANET and development of proposed systems and implementation would increase safety among road users and improve the comfort for the corresponding passengers, drivers and also other road users, and a great improvement in the traffic efficiency would be achieved. This research paper investigates the current and existing security issues associated with the VANET and exposes any slack amongst them in order to lighten possible problem domains in this field.

Keywords

Vehicular Ad Hoc Network (VANET), MANET, Vehicle-to-Vehicle (V2V) Communication, Vehicle-to-Infrastructure (V2I) Communication

1. Introduction

The road has become a "moving network", today vehicles are been designed to carry networks, communicate with other vehicles via a communication link or channel. The 2009 Urban Mobility Report, issued by the Texas Transportation Institute, reveals that in 2007, the congestion caused Urban Americans to travel 4.2 billion hours more and to purchase an extra 2.8 million gallons of fuel [1] [2]. This caused a great cost of 187.2 $billion and an increase of 50% and above in the previous decade [1] [2].

Recently, the attention of institutes and industries on VANET has grown vastly due to the promising features. The communication between vehicles has created a research field that can enhance the security and the effi-

How to cite this paper: Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Networks (VANET). *Int. J. Communications, Network and System Sciences*, **8**, 552-566.
http://dx.doi.org/10.4236/ijcns.2015.813050

ciency of transportation system, traffic conditions and also non-safety measures like weather information, location etc. [3]-[5].

According to configuration of network, VANET can be divided into three categories namely: Wireless Wide Area Network (WWAN), Hybrid Wireless Architecture, and Ad Hoc V2V communication. In the WWAN, the access point of the cellular gateway are fixed, this allows the direct communication between the vehicle and the access point. The Hybrid wireless Architecture uses WWAN access points at some points in the network, while the communication between those access points in the Hybrid Wireless Architecture are achieved with the use of Ad Hoc communications. The third category is the Ad Hoc Vehicle-to-Vehicle communication; this doesn't require any fixed access point for the vehicles to communicate. Vehicles are designed with their own wireless network card and the setting up of an Ad Hoc network can be actualized for each vehicle.

VANET is a subsystem of Mobile Ad Hoc Network (MANET), VANET communicates with the MANET-like technology with the equipment nearby along the road side, and also to communicate between vehicles. Their characteristics are different from that of other networks [3]-[5]. Unavailability of road information can create a possibility of accurately stating the position of the vehicle at that time. The vehicle is the node in VANET and the nodes are limited to a particular type of topology while in motion which is the road topology. The nodes can provide power for data processing and information transmission to sustain the functioning of the node [4]-[6].

Although VANET possess the characteristics of a wireless network, there's a unique character that is associated to the mobility and the unreliable channel condition [6] [7]. Besides the safety application that VANET provides for the road users, there's also the access to multimedia, mobile e-commerce, weather information etc. [6]-[8]. There are some applications that are specifically designed to aid drivers and improve the services of VANET such as: Advance Driver Assistance System (ADASE2), Crash Avoidance Matrices Partnership (CAMP), NOW (Network on Wheels), Fleet Net, etc. these applications were designed and developed with the joint services of different government and some major car manufactures company [8]-[10].

The paper will discuss about the Vehicular Ad Hoc Networks (VANET) in detail in the Section 2 and discussing about main architecture of VANET in the Section 3. The Section 4 discusses about different classifications of VANET applications and Section 5 discusses about main characteristics of VANETs. The common VANET units and entities in classification of environment are discussed in Section 6. The VANET communications patterns are classified and explained in 3 main categories as warning broadcast, group communication and beaconing in Section 7. The routing features of VANETs which are geocast, broadcast, unicast and multicast is discussed in Section 8 in detail. In Section 9, security issues discussed which are based on three main categories such as: availability, authenticity, and confidentiality and research is concluded with Section 10.

2. Vehicular Ad Hoc Network (VANET)

Vehicular Ad Hoc Network (VANET) utilizes cars as a mobile node to create a mobile network [13]. Vehicles act as a mobile node with the corresponding network. The basic aim of VANET is to improve and increase the safety on our roads and road users, comfort of passengers, and also aid the communication between vehicles and roadside equipment. The VANET communication medium is installed on each node (vehicle) [11]. As shown in **Figure 1**, each vehicle has its own communication wireless network card which allows ease of communication flow between vehicles and roadside units.

Figure 2 Shows the different domains that exist in VANET. The Mobile Domain consists of (Vehicle and Mobile Devices) such as PDA, Smart Phones, and Laptop etc. The Generic Domain consists of (Internet Infrastructure and Private Infrastructure) such as nodes and servers. While the Infrastructure Domain consists of (Road Infrastructure or Units and the Central Infrastructure) such as the RSU that communicate with the vehicle along the road, and the management center that communicates with the internet.

The Mobile Domain communicates with the Infrastructure Domain and the Infrastructure Domain communicates with the Generic Domain and data flows between the different domain to provide effective and efficient use of the road by the road users.

Since the communication is provided in 2 different way in VANET, there are some fixed node that act as a roadside unit or equipment which enables the ease of VANET to serve as a gateway to the internet and also in accessing geographical data [12]-[14]. Each node in the VANET doesn't only participate in data transmission and receiving, they also act as a wireless router of the network as different nodes communicate via their own

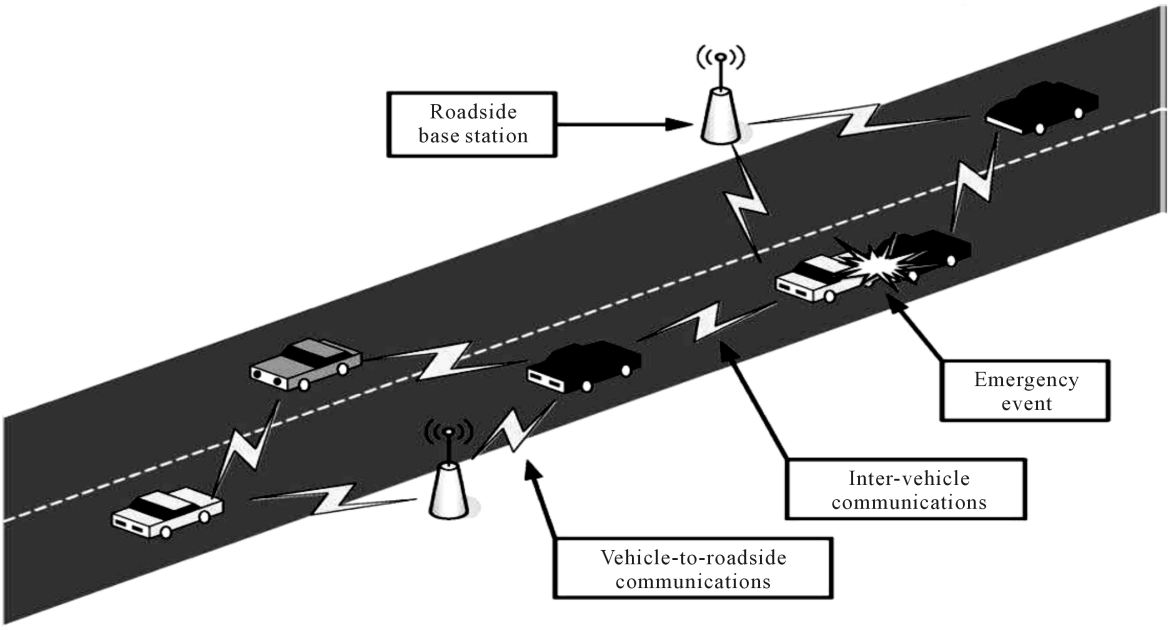

Figure 1. A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give the drivers the time to react to life-endangering events.

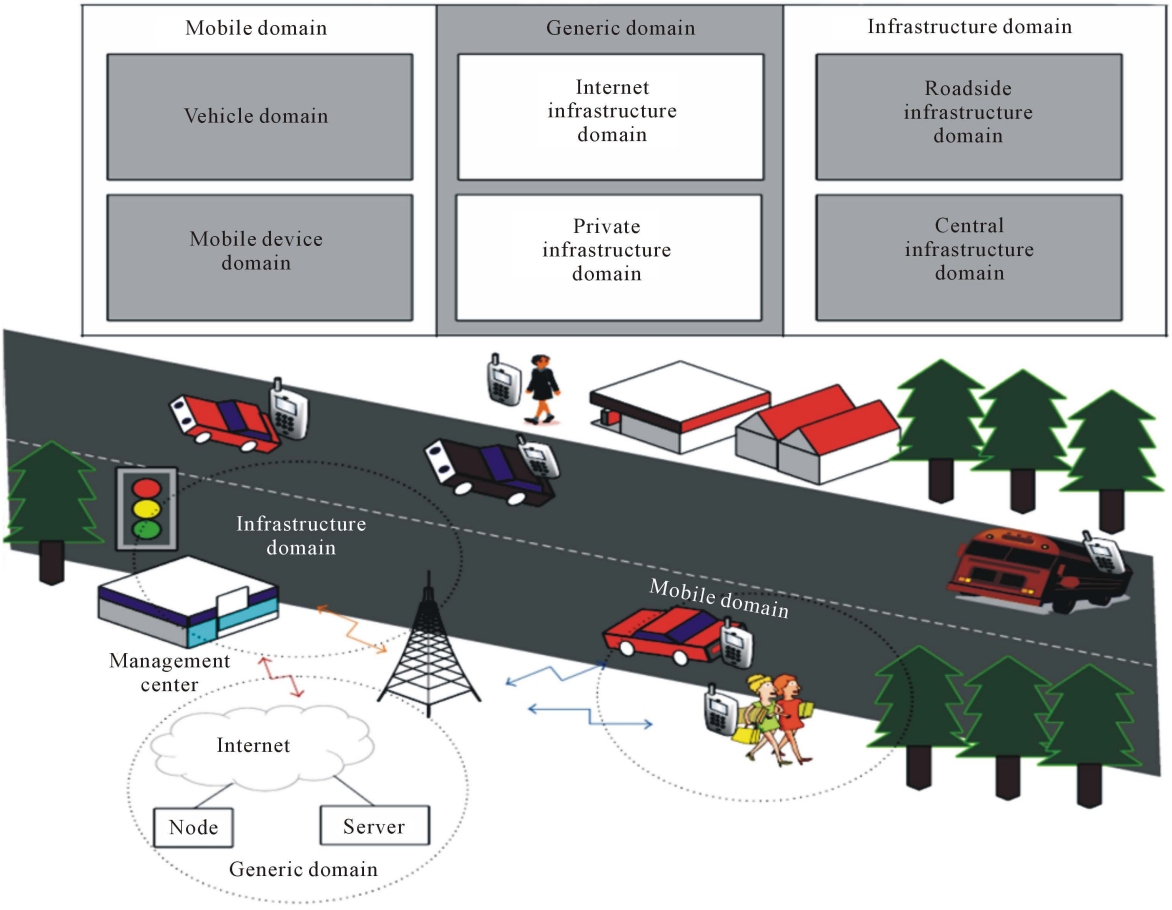

Figure 2. VANET system sphere.

communication range, permitting cars in the region of 100 to 300 meters of each other to join the network, and create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created [15].

Components of VANET are onboard units and roadside units as shown in **Figure 3**, we can see how communication is transmitted from the roadside unit to the onboard unit in the vehicle, and also a vehicle to vehicle communication. This creates a better share of information between vehicles.

VANET, vehicles act as nodes, unlike MANET that vehicles are set to move on a predefined road. The vehicles must follow traffic signs and signals and their velocity relies on the speed sign [9]. Wireless devices such as; Personal Digital Assistant (PDA), Remote Keyless Entry Device, Mobile Phones, Laptops etc. are supported by VANET inside the vehicle [16]-[20]. Due to the increase of mobile wireless devices, the demand for the vehicle-to-vehicle (V2V), vehicle-to-roadside (VRC), and vehicle-to-infrastructure (V2I) communication will grow rapidly [20]. There are two type of communication infrastructure available by the VANET; first is the wireless ad hoc network, where there's communication between vehicles without infrastructural support. Secondly, the communication between the vehicle and the road side unit [14]. The IEEE defined standard of establishing a VANET is 802.11 or 802.16 (WIMAX).

Due to the relatively high speed of nodes (vehicles) in the VANET and the clustering of vehicles in a particular location can cause a very large network at that time due to the independency of each node, a communication standard known as the Dedicated Short Range Communication (DSRC) was developed to fix the issue. This communication standard clearly requires the use of Road Side Units (RSUs) that are installed along the road as gateways between the infrastructure and the nodes (vehicles) and also in reverse [21]. The DSRC communicates on a 5.9 GHZ band and uses 802.11 access methods. USA allocated 75 MHZ of spectrum in the 5.9 GHZ, while Europe allocated 30 MHZ of spectrum in the 5.9 GHZ band for DSRC, this is to be utilized by the Intelligent Transportation Systems (ITS) [22].

As shown in **Table 1**, there are 7 MHz wide channels. Four of which are service channels that is used for safety and non-safety applications, and there is a control channel (CCH) which is used to control the channel. The two reserved channel (172 and 178) respectively are for future safety applications. Channel 172 is reserved for high accessibility and low inactivity of applications while channel 178 is reserved for high power public safety applications.

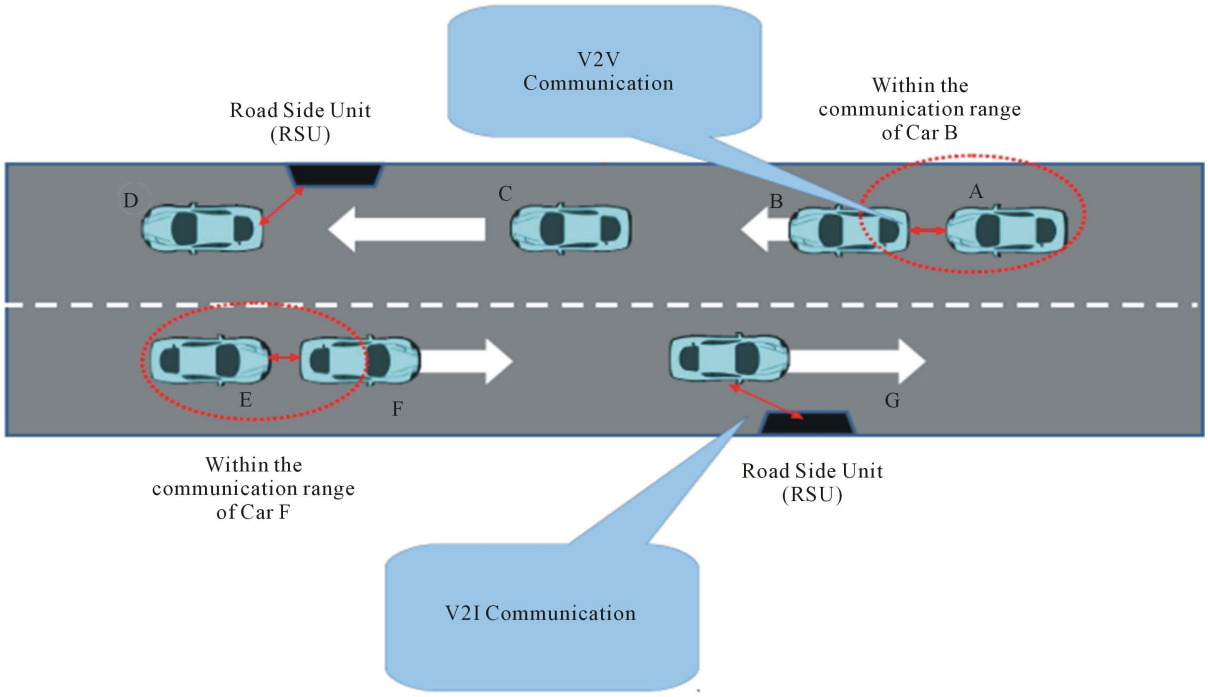

Figure 3. Typical components of VANET.

3. Layered Architecture for VANET

The OSI model group similar communication functions into one of the seven logical layers [23]-[25]. In VANET, the session and the presentation layers are omitted and a particular layer can be further broken or partitioned into sub layers in the VANET architecture, as illustrated in **Table 2** below [25]. The architecture of VANET may change in different regions, and the protocols and interface will also be different. As shown in **Table 3**, the protocol stacks for the Dedicated Short Range Communication (DSRC) in the US [26]. At various layers, different protocols are designed to be used of which some are still under development [26].

The approved amendment to the IEEE 802.11 standard which is IEEE 802.11p standard adds a wireless access in VANET vehicular environment (WAVE). This is focused primarily on the physical layer and MAC sub layer of the protocol stack. The IEEE 1609 standard is a higher protocol standard compared to the IEEE 802.11p. The IEEE 1609 standard functions in the middle layers of the protocol stack and it adaptably supports the safety applications in VANET. While the nonsafety applications are supported through a different set of protocols. The Network, Transport layer services for the nonsafety applications in VANET are supported or provided by IPV6, TCP, and UDP [27]-[29].

Table 1. DSRC spectrum allocation.

Name	MHz Wide Channels Number	Spectrum Allocated (GHz)
Critical Safety of Life (Reserved)	172	5.860 GHz
Service Channel (SCH)	174	5.870 GHz
Service Channel (SCH)	176	5.880 GHz
Control Channel (CCH)	178	5.890 GHz
Service Channel (SCH)	180	5.900 GHz
Service Channel (SCH)	182	5.910 GHz
High-Power Public Safety (Reserved)	184	5.920 GHz

Table 2. The OSI model in VANET.

Application Layer	
Transport Layer	
Network Layer	
Link Layer	LLC Sublayer
	MAC Sublayer
Physical Layer	PLCB Sublayer
	PMD Sublayer

Table 3. The layered architecture for DSRC.

Safety Applications	**Nonsafety Applications**
Transport and Network Layer IEEE 1609.3	Transport Layer TCP/UDP
Security IEEE 1609.2	Network Layer IPV6
LLC Sublayer IEEE 802.2	
MAC Sublayer IEEE 1609.4	
MAC Sublayer	IEEE 802.11 p
Physical Layer	

4. VANET Applications

There are two categories of applications that is associated with the VANET; safety and user based applications [30].

4.1. Safety Related Applications

The safety related applications are used to increase safety on the road and also that of the road users, such applications are: collision avoidance, cooperative driving, and traffic optimization.

Collision Avoidance: Some studies states that 60% of road accidents can be avoided if the drivers are warned 0.30 seconds before the collision occurs [31]-[33]. In the collision avoidance application, a signal or a nodes location is broadcasted to other nodes if an accident occurs so as to prevent other vehicles coming to get involved.

Cooperative Driving: An uninterrupted/safe journey can be achieved via traffic related warning signals such as changing of lane, the speed limit, negotiating a bend or curve etc. drivers are practically responsible and involved in this application, because many accidents occurs because of the lack of cooperation between drivers [34] [35].

Traffic Optimization: Vehicles acts as data collectors for the VANET. A signal like (JAM, ACCIDENT) etc. can be sent among the vehicles when there's a disruption on the road involving a vehicle or more so they can choose an alternative route to optimize the traffic and save time. For example, if there's a congestion on one lane the information can be transmitted or relayed to the vehicle on the opposite lane so it can be delivered faster to vehicles heading towards the congestion location. This gives enough time to for the vehicles approaching to choose an alternate route [36].

4.2. User Based Applications

Safety comes first in the usage of the road, afterwards other services can be included. Infotainment (Information and Entertainment) services is also provided by VANET, such as:

Peer-to-Peer Application: these application can be utilized usefully to provide music, video, etc. sharing among the vehicles in the network.

Internet Connectivity: VANET provides the road users with internet connectivity

Other Services: Geographical locations, payment services, etc. are provided by non-safety applications in VANET.

5. Characteristics of VANET

As earlier stated VANET is a sub of MANET, but it has its own distinguished characters such as:

High Mobility: Because vehicles move at high speed it is difficult to predict a node position and also it makes protection of nodes privacy hard.

Rapid Changing Network Topology: Due to the random speed of a node (vehicle), node position is difficult to ascertain and its position changes frequently, this causes the network topology to change frequently in VANET.

Unbounded Network Size: VANET network size is not limited to a particular region or locality, it can be implemented for a city or more, or even for countries. VANET is geographically limitless.

Frequent Exchange of Information: Information can be exchanged amongst vehicles and road side units (RSUs) die to the AD Hoc nature of VANET. This makes the information exchange more frequent and updated.

Wireless Communication: The technology that VANET runs on is a wireless technology, therefore nodes are connected and information exchange are done via a wireless communication channel.

Time Critical: Time limits are set on each information packet that is been sent or received, this enables the delivery of information at the right time to avoid unwanted delays and decisions can be made accordingly by the corresponding node with action taken.

Sufficient Energy: The nodes have huge power source, because the vehicles run on their own battery. There's no limited power supply for the corresponding components to function properly. This cause demanding techniques to be used by VANET, such as RSA, ECDSA etc.

Better Physical Protection: Because VANET nodes are vehicles, it's more secured physically. This makes VANET nodes to be more difficult to compromise physically and also reduce physical attack on the infrastructure.

6. VANET Model

In VANET there are different units involved in the deployment. Although majority are nodes (Vehicles), there are other units or entities that keep the basic operations functioning in the network. Due to the large and complex system model, it has been categorized into four sub models namely: Driver and Vehicle Model, Traffic Flow Model, Communication Model, and application Model [37]-[39].

Driver and Vehicle Model: This shows the behavior of a single vehicle. In this model two factors are considered such as: different driving styles and the vehicle characteristics. Example a violent driver or passenger and a sport car [39].

Traffic Flow Model: This model depicts the interaction between vehicles, drivers, and the infrastructure to develop a good road network [39] [40].

Communication Model: This shows the flow of data or information between or among the road users [41].

Application Model: This points out the usefulness in the behavior and quality of cooperative VANET applications [41].

Figure 4 illustrated the VANET units and entities that makes up the VANET model, and it is explained in detail section below.

6.1. Common VANET Units and Entities

There are two different environments generally researched in VANET namely; Infrastructure and Ad-Hoc environment.

6.1.1. Infrastructure Environment

In this environment, units or entities can be interconnected permanently. Inside this environment mainly contains the entities that mange traffic and also gives access to external services. Manufactures are known to be inside this environment of the VANET model; because during manufacturing they identify each vehicle uniquely. Legal authority is also in this environment of VANET model; putting aside the different regulations that binds countries, vehicles registration and offence reporting is ensured. The Trusted Third Party (TTP) are also in this environment [42]. They offer various services such as time stamping and credential management. Manufactures and the Authority are related to (TTP) because the services are needed, example; issuing of electronic credentials [42]. Service providers are also in this environment, because they give out services that can be accessed via the VANET, such services are' Location Based Services (LBS) or Digital Video Broadcasting (DVB) etc. [42].

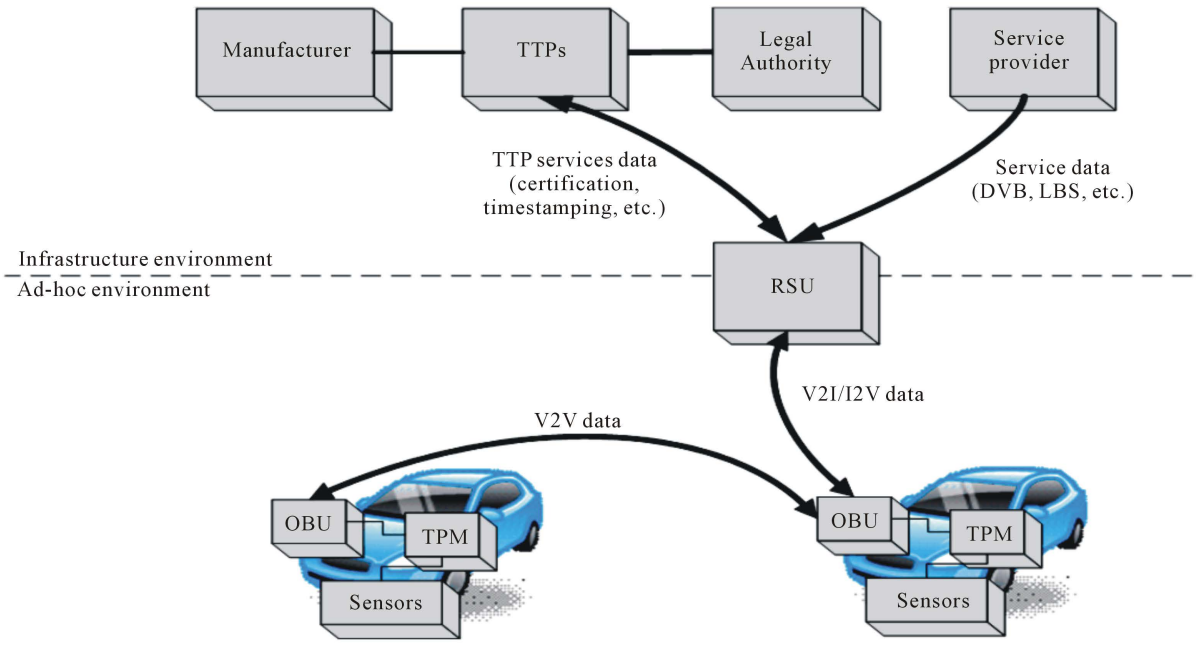

Figure 4. VANET units and entities.

6.1.2. Ad-Hoc Environment

This environment creates ad-hoc communications from vehicles. The vehicles are equipped with 3 different devices namely; On-Board Unit (OBU) that enables the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication [23]. The Ad-Hoc environment also have a set of sensors to their status and its environment e.g. (Fuel Consumption, Slippery Road, and Safety Distance). The data gotten can be shared among other node to improve and increase road safety.

A Trusted Platform (TPF) is always installed on the vehicles, such devices are for security purposed and also for computation and reliable storage [43].

7. VANET Communication Patterns

The use of VANET enables the use of several applications from safety to non-safety applications. These applications exchange messages over VANETs and they are used for different proposes. In the VANET they are four different communication pattern identified [44] [45]. Although other communication pattern exists such as (multimedia access, location based services, etc.).

7.1. Vehicle-to-Vehicle (V2V) Warning Broadcast

This communication pattern is useful in a unicast or multicast situation, where message is been sent to a specific or a group of vehicles. For example and emergency vehicle is approaching, a message can be sent to vehicles coming; this will create an easy passage for the emergency vehicle, or when an accident is detected, a message can be sent to arriving vehicles to warn them and also increase safety on the road [46]. This is shown in **Figure 5** below.

7.2. Vehicle-to-Vehicle (V2V) Group Communication

In this communication pattern, only vehicles that share similar features can participate in the communication. Such features can be static or dynamic in nature, that is vehicles of the same manufacture or enterprise (static nature) or vehicles that appears to be in the same area in a particular time interval (dynamic nature) [47] [48]. This is shown in **Figure 6** below.

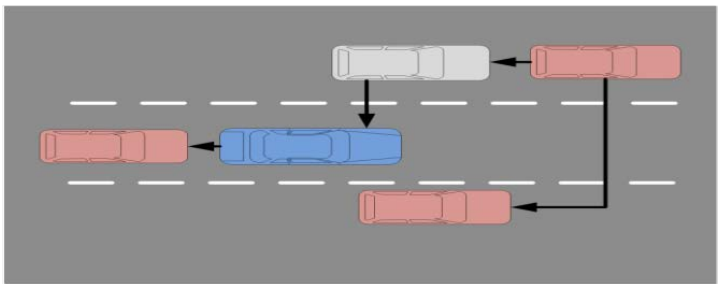

Figure 5. V2V warning broadcast.

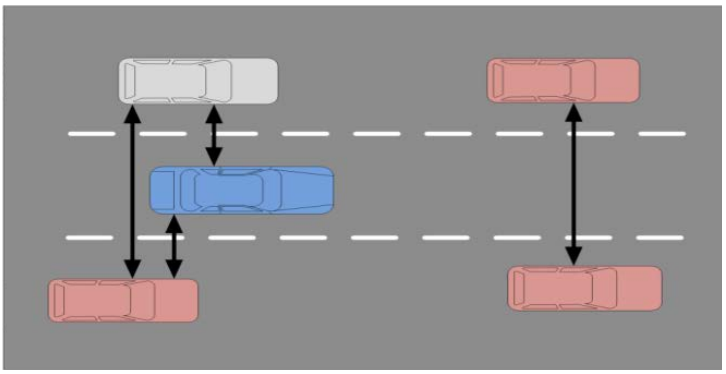

Figure 6. V2V group communication.

7.3. Vehicle-to-Vehicle (V2V) Beaconing

Under this pattern, messages are sent periodically to vehicles that are nearby. These messages contain breaking use, heading, current speed, bend negotiation etc. of the sender or transmitting vehicle. As shown in **Figure 7**, the V2V beaconing communication messages are only sent to 1-hop communication vehicle that is the messages are not forwarded after receiving. This is helpful because the message enables vehicles to discover and access the best neighbor to route a message through or to [49]-[51].

7.4. Infrastructure-to-Vehicle/Vehicle-to-Infrastructure Warning

Messages are relayed either from the infrastructure Road Side Units (RSUs), or from a vehicle to RSUs when a vehicle or RSU spots a potential danger. For example a warning message can be sent from or by the RSU to approaching vehicles heading towards an intersection that a possible collision could happen. This communication pattern is very useful for enhancing road safety [52] [53]. **Figure 8** shows how a warning message was communicated to various nodes to avoid collision.

8. Routing in VANET

In the past few years, routing in VANET have been researched widely [42] [52]-[54]. However, due to the characteristics of VANET having a high active topology recurrent connectivity, the commonly used routing protocols that were implemented for MANET have been tested and evaluated for use in VANET environment [55]. Depending on the number of sending and receiving nodes involved, the routing in VANET can be classified into three types namely; Geocast/Broadcast, Multicast, and Unicast approaches.

8.1. Geocast/Broadcast

This protocol is very important in VANETs. In [56], the review of various geocast/broadcast protocols on VANET was researched on, such as:

- Spatially Aware Packet Routing Algorithm (this protocol is able to predict holes in topology and conduct the geographical forwarding).
- SHDV (this protocol helps find the best path to forward a packet through).

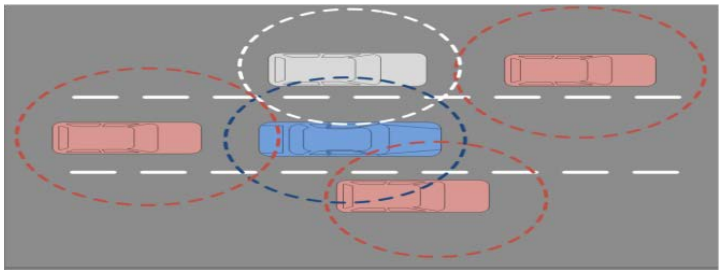

Figure 7. V2V beaconing.

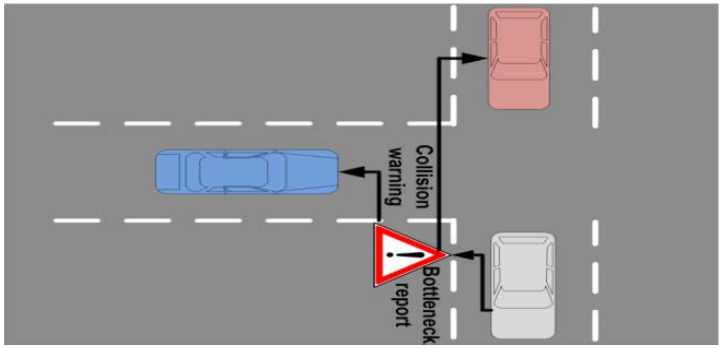

Figure 8. I2V/V2I warning.

- Interface Awake Routing Scheme (this enables the node with a multichannel radio interface and switches the channel based on the SIR evaluation).
- FROV (this selects the retransmission and spans further node to rebroadcast a message).
- Multi-hop Broadcast Protocol (this protocol segments the road and choose the vehicle that is far in a non-empty segment).

Other protocols such as; V-TERADE, UMB, AMB, MHVB, and MDDV have been proposed by other researchers [56].

8.2. Multicast Protocol

Multicast is important among communication between group of vehicles in some vehicular situations such as; road blocks, high traffic density or congestion, accidents, road intersections, bad road surface condition etc. In [56], the multicast protocol was divided into two types, 1) topology based approaches such as ODMRP (this generates a source based multicast mesh and forwards it based on the group address), MAODV (this generates a group based multicast tree), and GHM (this generates group-based multicast meshes). 2) location-based approaches, such as PBM (which is based on positions of all 1-hop neighbors and also that of individual destinations), SPBM (this introduces hierarchal group membership management), LMB (this uses the multicast region as destination information for multicast packets), and RBM and IVG (which define a multicast scope for safety warning messages).

8.3. Unicast Protocol

The unicast communication protocol for VANET is in three ways (as shown in **Table 4**):

- Greedy: in this protocol, nodes forward packets to the vehicle or nodes that are far off neighbor coming towards their destination, like (GYTAR).
- Opportunistic nodes use “carry-toward” technique, where this is done in order to resourcefully deliver the data to the corresponding destination, just like the topology-assist, geo-opportunistic routing etc.
- Trajectory Based: Nodes compute the paths that will possibly lead to the destination and deliver the data by relaying it to nodes that are along one of the computed paths, just like the trajectory-based data forwarding (TBD) [55] [56].

9. VANET Security Issues

Security is always a challenge for any infrastructure that is been used in communication. Safety in VANET is of high priority because human lives are involved. The security challenges or issues must be put in place during the design of VANET architecture [53]-[55]. In [56], the author classified attackers into three categories or dimensions; insider versus outsider, malicious versus rational, and active versus passive.

In VANET security issues, the threats are based into three main groups such as; availability, authenticity, and confidentiality. The following 3 subsections expose these issues in details.

9.1. Threats to Availability

The threats to availability of vehicle-to-vehicle and vehicle-to-roadside communication are:

1) Denial of Service Attack: this kind of attack can be done or carried out by an insider, and or outsiders in the network, such attack causes the network to be unavailable to the authentic users. Flooding and jamming with a high volume generated artificial messages causes the VANET components such as the nodes onboard units and roadside units not to sufficiently process the overload caused by the DoS attack.

2) Broadcast Tampering: This attack is carried out by an insider. It inputs false safety messages into the VANET to inflict damage or harm to the road users. An accident can occur when attacker manipulates the traffic on a specific route.

3) Malware: Virus or works can cause serious interference of flow of operation if introduced into VANET. This attack is often carried out by insiders more than outsiders and also it can be downloaded into the network when a firmware update is done.

4) Spamming: Spam messages in VANET can lead to increased transmission inactivity. This is more difficult to control because there’s no centralized administration.

Table 4. Unicast protocols and algorithms in VANET.

	Protocols/Algorithms	Main Ideas
GREEDY	Geographical source routing (GSR)	Determines the destination location by RLS (reactive location service)
	Greedy perimeter geographic routing (GPCR)	The packet is greedily forwarded to the junction node (coordinator)
	Improved greedy traffic-aware routing (GyTAR)	Selects junctions based on vehicles traffic density and distance to the destination
	Connectivity-aware routing (CAR)	1) Greedy forwarding between anchor points along the selected path 2)The packet is forwarded to a node closer to an anchor point
OPPORTUNISTIC	OPERA: Opportunistic Packet Relaying in disconnected vehicular ad hoc networks	1) Vehicles moving in the same direction are grouped into clusters 2) Opportunistic technique is used to select a better available path
	Topology-assist geo-opportunistic routing	Uses two-hop beacons for the selection of a forwarding node
	MaxProp	1) Uses packet priorities to maximize delivery 2) Includes three stages: neighbor discovery, data transfer, and storage management
	SiFT	A data forwarder selection decision is shifted from the sender to receiver
TRAJECTORY	Geographical opportunistic routing (GeOpps)	A data forwarder is selected based on the trajectory information of individual vehicles
	Trajectory-based data forwarding (TBD)	Is based on vehicle trajectory information and traffic statistics
	Two-level trajectory-based routing (TTBR)	1) The communication area is divided into cells of a grid 2) A grid based location system is applied where some peer servers are distributed

5) Black Hole Attack: This form of attack is cause by nodes refusing to participate in the network or when a node drops out of the network, when this happens all communication routes and link it had before would be broken, this causes a failure in broadcasting message.

9.2. Threats to Authenticity

In VANET authenticity provision is very important. This includes the protecting of legitimate node from the attackers "insider or outsider" infiltrating the network with fake identifies, such threats are:

1) Masquerading: This attack is different from others and it's easier to carry out. The attacker joins the network by having to get a functioning onboard unit and the attacker possess as a legitimate vehicle in the network, variety of attack can be carried out or feasible such as creating of false message and forming of black holes.

2) Global Positioning System (GPS) Spoofing: Global positioning system keeps a location table that holds the geographical locations of all vehicles on the network and their identities. An attack can be carried out using the GPS spoofing through GPS satellite simulator to create a false location on the GPS system in the network, thereby causing the vehicle to think that the corresponding location is the right one. This is because the GPS satellite simulator can generate signals that are way stronger than that generated by the authentic or real satellite.

3) Replay Attack: In this attack, the attacker reinsert packets that have been previously used by nodes into the network, this can poison a node's location table by replaying bacons. Although VANET that operate in the WAVE framework are protected from this attack, but to continue protection a precise source of time should be kept and organized because it is used to keep cache of recently received messages in contrast of the incoming messages.

4) Tunneling: An attacker utilizes the momentarily loss of a vehicle positioning system when it goes through a tunnel before resurfacing on the other side to receive its positioning information. The attacker quickly injects

false positioning information or data in to the onboard unit of the node, causing the node to assume that the information received is valid.

5) Position Faking: In VANET, vehicles are responsible for the detailing of their own position or location information. This makes impersonation nearly impossible. Unsecured communication link or channel can create a blind spot where attackers can quickly modify or falsify their own position or that of other vehicles, create additional identities also known as (Sybil Attack), or even block vehicles from receiving and relaying vital and authentic safety messages.

6) Message Tampering: In this attack, the attacker alters or modify the message that's been relayed or exchanged from vehicle-to-vehicle or vehicle-to-roadside unit communication in order to forge application request or response from other nodes.

7) Message Suppression/Fabrication/Alteration: The attacker physically disables the communication link between vehicles or modifies the application so that the vehicle cannot send or receive or respond to application beacons.

8) Sybil Attacks: In VANET, periodic messages are 1-hop broadcast, this is for securing the physical layer. When the network is not secured an attacker can partition the network and make delivery safety message impossible.

9.3. Threats to Confidentiality

Messages that are exchanged between nodes (vehicles) in VANET are open to confidentiality threats or attack with techniques such as illegitimate collection of messages through eavesdropping and passive attacks which are stated in the literature by the researchers.

10. Conclusions

VANET is an area of research that holds promising future and for vehicular users. However, it has its own challenges in the security prospect. VANET aims at reducing the accidents on our roads and increasing the flow of information among vehicle and the road users. The unique nature of VANET springs up issues like illegal tracking and jamming of the network. In this paper, we introduced VANET, its architecture, components, communication pattern and issues in its security. In the course of this research, we found out the routing protocols used in VANET that enabled road users to communicate and receive messages appropriately, such as: Geocast/ Broadcast, Multicast, and Unicast protocol. Also VANET communication pattern, entities and characteristics which include: High Mobility, Rapid Changing, Network Topology, Unbounded Network Size, Frequent Exchange of Information, Wireless Communication, Time Critical, Sufficient Energy and better Physical Protection. The characteristics of VANET expose the usability and efficiency in VANET.

With more research done on the security issues of VANET, I believe that VANET will cause a technological change and improvement for the road users. Useful information exchange can prevent future damage and accidents on our road. Future research would be conducted on comparing the various data security mechanisms and their performance metrics.

References

[1] Kadum, A. (2013) A Survey on Vehicular Ad Hoc and Sensor Networks (VASNET).

[2] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **3**, 79-94. http://dx.doi.org/10.5121/ijasuc.2012.3306

[3] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003

[4] Sivasakthi, M. and Suresh, S. (2013) Research on Vehicular Ad Hoc Networks (VANETs): An Overview. *Journal of Applied Sciences and Engineering Research*, **2**, 23-27.

[5] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications, Society for Science and Education, United Kingdom*, **2**, 1-6.

[6] (2011) Vehicular Ad Hoc and Sensor Networks—Principles and Challenges. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing* (*IJASUC*), **2**.

[7] Li, F. and Wang, Y. (2007) Routing in Vehicular Ad Hoc Networks: A Survey. *IEEE Vehicular Technology Magazine*, **2**, 12-22.

[8] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad Hoc Networks. *International Journal of Science and Advanced Technology*, **2**, 188-191.

[9] Li, F. and Wang, Y. (2007) Routing in Vehicular Ad Hoc Networks: A Survey. *IEEE of Vehicular Technology Magazine*, **2**, 12-22. http://dx.doi.org/10.1109/MVT.2007.912927

[10] Saha, A.K. and Johnson, D.B. (2004) Modelling Mobility for Vehicular Ad Hoc Networks. *ACM International Workshop on Vehicular Ad Hoc Networks*, Philedelphia, 91-92.

[11] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications, Network, and System Sciences*, **7**, 365-372. http://dx.doi.org/10.4236/ijcns.2014.79038

[12] Manvi, S.S., Kakkasageri, M.S. and Mahapurush, C.V. (2009) Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols in Vehicular Ad Hoc Network Environment. *International Conference on Future Computer and Communication*, Kuala Lumpar, 3-5 April 2009, 21-25.

[13] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. *Proceedings of the* 6*th International Conference on Security of Information and Networks* (*SIN* '13). Aksaray, 26-28 November 2013, 454-456. http://dx.doi.org/10.1145/2523514.2523586

[14] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 5*th International Conference on Computational Intelligence, Communication Systems and Networks* (*CICSyN*), Madrid, 5-7 June 2013, 334-337. http://dx.doi.org/10.1109/cicsyn.2013.79

[15] Bernsen, J. and Manivannan, D. (2008) Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service. *The* 4*th International Conference on Wireless and Mobile Communications*, Athens, 27 July-1 August 2008, 1-6. http://dx.doi.org/10.1109/icwmc.2008.15

[16] Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N. and Nemoto, Y. (2007) A Stable Routing Protocol to Support ITS Services in VANET Networks. *IEEE Transactions on Vehicular Technology*, **56**, 3337-3347. http://dx.doi.org/10.1109/TVT.2007.906873

[17] Sari, A. (2014) Economic Impact of Higher Education Institutions in a Small Island: A Case of TRNC. *Global Journal of Sociology*, **4**, 41-45.

[18] Hartenstein, H. and Laberteaux, K.P. (2008) A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Communication Magazine*, **46**, 164-171.

[19] Sari, A. and Onursal, O. (2013) Role of Information Security in E-Business Operations. *International Journal of Information Technology and Business Management*, **3**, 90-93.

[20] Eichler, S., Ostermaier, B., Schroth, C. and Kosch, T. (2005) Simulation of Car-to-Car Messaging: Analyzing the Impact on Road Traffic. *IEEE ASCOTS*, 507-510.

[21] Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *International Journal of Communications, Network and System Sciences*, **8**, 29-42. http://dx.doi.org/10.4236/ijcns.2015.83004

[22] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. http://dx.doi.org/10.4236/jis.2015.62015

[23] Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, **8**, 260-273. http://dx.doi.org/10.4236/ijcns.2015.87026

[24] Gerlach, M. (2006) Full Paper: Assessing and Improving Privacy in VANETs. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=84FC4EF0852B23FBF15CF35E16E0450D?doi=10.1.1.84.8167&rep=rep1&type=pdf

[25] Dahiya, A. and Chauhan, R. (2010) A Comparative Study of MANET and VANET Environment. *Journal of Computing*, **2**.

[26] Sesay, S., Yang, Z. and He, J.H. (2004) A Survey on Mobile Ad Hoc Network. *Information Technology Journal*, **3**, 168-175. http://dx.doi.org/10.3923/itj.2004.168.175

[27] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. 2013 *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering* (*TAEECE*), Konya, 9-11 May 2013, 579-582. http://dx.doi.org/10.1109/TAEECE.2013.6557339

[28] Toor, Y., Muhlethaler, P. and Laouiti, A. (2008) Vehicle Ad Hoc Networks: Applications and Related Technical Issues. *IEEE Communications Surveys & Tutorials*, **10**, 74-88. http://dx.doi.org/10.1109/comst.2008.4625806

[29] Sari, A., Rahnama, B. and Caglar, E. (2014) Ultra-Fast Lithium Cell Charging for Mission Critical Applications. *Transactions on Machine Learning and Artificial Intelligence*, **2**, 11-18. http://dx.doi.org/10.14738/tmlai.25.430

[30] Hu, Y.-C. and Laberteaux, K. (2006) Strong Security on a Budget. Wksp. Embedded Security for Cars. http://www.laberteaux.org/papers/vanet08-epidemic.pdf

[31] Raya, M. and Hubaux, J. (2005) The Security of Vehicular Ad Hoc Networks. *Proceedings of the* 3*rd ACM Workshop on Security of Ad Hoc and Sensor Networks* (*SASN* 2005), Alexandria, 7-10 November 2005, 11-21. http://dx.doi.org/10.1145/1102219.1102223

[32] Robinson, C.L., Caminiti, L., Caveney, D. and Laberteaux, K. (2006) Efficient Coordination and Transmission of Data for Cooperative Vehicular Safety Applications. *In VANET*'06: *Proceedings of the* 3*rd International Workshop on Vehicular Ad Hoc Networks*, New York, 10-19.

[33] Sari, A. and Mahmutoglu, H. (2013) Potential Issues and Impacts of ICT Applications through Learning Process in Higher Education. *Procedia—Social and Behavioral Sciences*, **89**, 585-592. http://dx.doi.org/10.1016/j.sbspro.2013.08.899

[34] Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R., *et al*. (2006) Attacks on Inter-Vehicle Communication Systems—An Analysis. *International Workshop on Intelligent Transportation*, Hamburg, 189-194.

[35] Buttyan, L. and Hubaux, J.-P. (2001) Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks. Swiss Federal Institute of Technology, Laussane.

[36] Sari, A. (2012) Impact of Determinants on Student Performance towards Information Communication Technology in Higher Education. *International Journal of Learning and Development*, **2**, 18-30. http://dx.doi.org/10.5296/ijld.v2i2.1371

[37] Callandriello, G., Papadimitratos, P., Lloy, A. and Hubaux, J.-P. (2007) Efficient and Robust Pseudonymous Authentication in VANET. *International Workshop on Vehicular Ad Hoc Networks*, Montreal, 9-14 September 2007, 19-28.

[38] Boneh, D. and Shacham, H. (2004) Group Signatures with Verifier-Local Revocation. *Proceedings of the* 11*th ACM Conference on Computer and Communications Security*, Washington DC, 25-29 October 2004, 168-177. http://dx.doi.org/10.1145/1030083.1030106

[39] Armstrong Consulting Inc. (n.d.). Dedicated Short Range Communications (DSRC) Home. Retrieved October 2009. http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[40] Sakib, R.K. and Reza, B. (2010) Security Issues in VANET.

[41] de Fuentes, J.M., González-Tablas, A.I. and Ribagorda, A. (2010) Overview of Security Issues in Vehicular Ad-Hoc Networks.

[42] Harsch, C., Festag, A. and Papadimitratos, P. (2007) Secure Position-Based Routing for VANETs. *Proceedings of IEEE* 66*th Vehicular Technology Conference*, *VTC*-2007, Baltimore, 30 September-3 October 2007, 26-30. http://dx.doi.org/10.1109/vetecf.2007.22

[43] Sari, A. (2014) Influence of ICT Applications on Learning Process in Higher Education. *Procedia—Social and Behavioral Sciences*, **116**, 4939-4945. http://dx.doi.org/10.1016/j.sbspro.2014.01.1053

[44] Sun, S., Kim, J., Jung, Y. and Kim, K. (2009) Zone-Based Greedyperimeter Stateless Routing for VANET. *Proceedings of International Conference on Information Networking*, *ICOIN* 2009, Chiang Mai, 21-21 January 2009, 1-3.

[45] Yu, D. and Ko, Y.-B. (2009) FFRDV: Fastest-Ferry Routing in DTN-Enabled Vehicular Ad Hoc Networks. *Proceedings of* 11*th International Conference on Advanced Communication Technology*, **2**, 1410-1414.

[46] Ali, S. and Bilal, S. (2009) An Intelligent Routing Protocol for VANETs in City Environments. *Proceedings of* 2*nd International Conference on Computer, Control and Communication*, *IC*4 2009, Karachi, 17-18 February 2009, 1-5. http://dx.doi.org/10.1109/ic4.2009.4909249

[47] Yang, J. and Fei, Z. (2013) Broadcasting with Prediction and Selective Forwarding in Vehicular Networks. *International Journal of Distributed Sensor Networks*, **2013**, Article ID: 309041. http://dx.doi.org/10.1155/2013/309041

[48] Chen, W., Guha, R.K., Taek, J.K., Lee, J. and Hsu, I.Y. (2008) A Survey and Challenges in Routing and Data Dissemination in Vehicular Ad-Hoc Networks. *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety* (*ICVES* '08), Columbus, 22-24 September 2008, 328-333.

[49] Wahid, A., Yoo, H. and Kim, D. (2010) Unicast Geographic Routing Protocols for Inter-Vehicle Communications: A Survey. *Proceedings of the* 5*th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wire Networks* (*PM2HW2N* '10), Bodrum, 17-21 October 2010, 17-24. http://dx.doi.org/10.1145/1868612.1868616

[50] Moustafa, H. and Zhang, Y. (2009) Vehicular Networks: Techniques, Standards, and Applications. CRC Press, Boca Raton. http://dx.doi.org/10.1201/9781420085723

[51] https://www.academia.edu/8721918/VANET_Vehicle_Ad_hoc_Networks

[52] http://en.wikipedia.org/wiki/OSImodel

[53] Hartenstein, H. and Laberteaux, K. (2010) VANET-Vehicular Applications and Inter-Networking Technologies. John Wiley & Sons, Hoboken.

[54] Maier, M.W., Emery, D. and Hilliard, R. (2004) ANSI/IEEE 1471 and Systems Engineering. *Systems Engineering*, **7**, 257-270. http://dx.doi.org/10.1002/sys.20008

[55] https://en.wikipedia.org/wiki/IEEE_802.11p

[56] Kosch, T., Schroth, C., Strassberger, M. and Bechler, M. (2012) Automotive Internetworking. Wiley, New York. http://dx.doi.org/10.1002/9781119944737